2007

Heron triangles with two fixed sides

Ionascu, Eugen J.

J. Number Theory 126 (2007), 52-68.
http://hdl.handle.net/10945/38856

Heron triangles with two fixed sides

Eugen J. Ionascu
Columbus State University
4225 University Avenue
Columbus, GA 31907
ionascu_eugen@colstate.edu

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán, México
fluca@matmor.unam.mx

Pantelimon Stănică
Naval Postgraduate School
Applied Mathematics Department
Monterey, CA 93943, USA
pstanica@nps.edu

October 8, 2006

Abstract

In this paper, we study the function $H(a, b)$, which associates to every pair of positive integers a and b the number of positive integers c such that the triangle of sides a, b and c is Heron, i.e., it has integral area. In particular, we prove that $H(p, q) \leq 5$ if p and q are primes, and that $H(a, b) = 0$ for a random choice of positive integers a and b.

1 Introduction

A *Heron triangle* is a triangle having the property that the lengths of its sides as well as its area are positive integers. There are several open questions concerning the existence of Heron triangles with certain properties. For example (see [6], Problem D21), it is not known whether there exist Heron triangles having the property that the lengths of all of their medians are positive integers, and it is not known (see [7] and [8]) whether there exist Heron triangles having the property that the lengths of all of their sides are Fibonacci numbers other than the triangle of sides $(5, 5, 8)$. A different unsolved problem which asks for the existence of a perfect cuboid; i.e., a rectangular box having the lengths of all the sides, face diagonals, and main diagonal integers has been related (see [11]) to the existence of a Heron triangle having the lengths of its sides perfect squares and the lengths of its angle bisectors positive integers (see [4] for more recent work).

Throughout this paper, we use the Vinogradov symbols $\gg$ and $\ll$ and the Landau symbols O and o with their usual meanings. We write $\log x$ for the maximum between the natural logarithm of x and 1. Thus, all logarithms which will appear are ≥ 1.

2 Heron triangles with two fixed prime sides

In this paper, we investigate (motivated by [2]) the Heron triangles with two fixed sides. Given a Heron triangle of sides a, b and c we write S for its area and $s = (a + b + c)/2$ for its semiperimeter. It is known that s is an integer and that $\min\{a, b, c\} \geq 3$. It is also known that if the triangle is isosceles, say if $a = b$, then c is even, and if we write h_c for the length of the altitude which is perpendicular on the side c, then h_c is an integer (see, for example, [12]). In particular, $(c/2, h_c, a)$ is a Pythagorean triple with a as hypothenuse.

Now let a and b be positive integers and let $H(a, b)$ be the number of distinct values of c, such that a, b and c are the sides of a Heron triangle. In this paper, we investigate the function $H(a, b)$.

We start with an easy proposition that finds some bounds for $H(a, b)$.

Proposition 2.1. *If $a \leq b$ are fixed, then $0 \leq H(a, b) \leq 2a - 1$.*

Proof. Apply the triangle inequality to obtain $c + a > b$ and $a + b > c$, which imply that $b - a < c < b + a$. The inequality on $H(a, b)$ follows. $\square$

Assume now that the prime power factorization of

$$n = 2^{a_0} p_1^{a_1} \cdots p_s^{a_s} q_1^{e_1} \cdots q_r^{e_r},$$

where $p_i \equiv 3 \pmod 4$ for $i = 1, \ldots, s$ and $q_j \equiv 1 \pmod 4$ for $j = 1, \ldots, r$. We let $d_1(n) = 0$ if any of the a_j with $j \geq 1$ is odd. Otherwise, let $d_1(n) = \prod_{j=1}^{r}(1 + e_j)$ be the number of divisors of n with primes among the q_i's. We shall need the following classical result (see, for instance, [1]).

Lemma 2.2. (i)[*Euler* (1738)] *A positive integer n can be represented as the sum of two squares if and only if $a_i \equiv 0 \pmod 2$ for all $i = 1, \ldots, s$.*
(ii) *Assume that $a_i \equiv 0 \pmod 2$ for all $i = 1, 2, \ldots, s$. The number of representations of n, say $r_2(n)$, as the sum of two squares ignoring order is given by $d_1(n)/2$ if $d_1(n)$ is even, and $(d_1(n) - (-1)^{a_0})/2$ if $d_1(n)$ is odd.*

Using Lemma 2.2, one can obtain a much better result than our previous Proposition 2.1. Let $\tau(n)$ stand for the number of divisors of the positive integer n.

Theorem 2.3. *If a and b are fixed, then $H(a, b) \leq 4\tau(ab)^2$.*

Proof. We start with the following observation. Let γ be any angle of a Heron triangle. Suppose that γ opposes the side c. Both $\cos\gamma$ and $\sin\gamma$ are rational, since $\cos\gamma = (a^2 + b^2 - c^2)/(2ab) \in \mathbb{Q}$ and $\sin\gamma = 2S/(ab) \in \mathbb{Q}$. Thus, if $\sin\gamma = u/v$, then $v = m^2 + n^2$ for some coprime integers m and n of opposite parities and $u \in \{2mn,\ |m^2 - n^2|\}$. Since a and b are fixed, in order to determine the number of Heron triangles that can be constructed using a and b, it suffices to determine the number of possible angles γ between a and b. Since $ab\sin\gamma = 2S \in \mathbb{Z}$, if $\sin\gamma = u/v$, then $v|ab$. For every divisor v of ab, the number of possible values for $\sin\gamma$ is given by twice the number of ways of writing $v = m^2 + n^2$ with coprime positive integers m and n, because for every such representation we may have $u = |m^2 - n^2|$ or $u = 2mn$. Furthermore, since when $\sin\gamma$ is fixed there are only two possibilities for γ, it follows that if $v|ab$ is fixed, then the number of values for γ is, by Lemma 2.2, at most $4d_1(v)$. Hence,

$$H(a, b) \leq 4 \sum_{v|ab} d_1(v) \leq 4\tau(ab) \sum_{v|ab} 1 \leq 4\tau(ab)^2.$$

$\square$

When a and b are prime numbers, we obtain a more precise result which improves upon [2].

Theorem 2.4. *If p and q are two fixed primes, then*

$$H(p,q) \text{ is } \begin{cases} = 0 & \text{if both } p \text{ and } q \text{ are } \equiv 3 \pmod 4, \\ = 2 & \text{if } p = q \equiv 1 \pmod 4, \\ \leq 2 & \text{if } p \neq q \text{ and exactly one of } p \text{ and } q \text{ is } \equiv 3 \pmod 4, \\ \leq 5 & \text{if } p \neq q \text{ and both } p \text{ and } q \text{ are } \equiv 1 \pmod 4. \end{cases}$$

Proof. Consider a Heron triangle of sides p, q and x. Let $s = (p+q+x)/2$ be its semiperimeter. By the Heron formula, its area is

$$S = \sqrt{s(s-p)(s-q)(s-x)}, \tag{1}$$

which after squaring becomes

$$16S^2 = 2p^2q^2 + 2p^2x^2 + 2q^2x^2 - p^4 - q^4 - x^4. \tag{2}$$

Since $\min\{p,q,x\} \geq 3$ and s is an integer, it follows that both p and q are odd primes and x is an even integer.

Assume first that the triangle is isosceles. Since both p and q are odd and x is even, we get $p = q$. Furthermore, $(x/2, h_x, p)$ is a Pythagorean triple. This shows that $p = u^2 + v^2$ with coprime positive integers u and v and $\{x/2, h_x\} = \{2uv, |u^2 - v^2|\}$. This leads to either $x = 4uv$, or $x = 2|u^2 - v^2|$. Hence, $H(p,p) \leq 2$. Furthermore, $H(p,p) = 0$ unless p is a sum of two squares, which happens precisely when $p \equiv 1 \pmod 4$.

Assume now that $2 < p < q$. Equation (2) is equivalent to

$$(p^2 + q^2 - x^2)^2 + (4S)^2 = (2pq)^2.$$

With $x = 2y$, the above equation can be simplified to

$$((p^2 + q^2)/2 - 2y^2)^2 + (2S)^2 = p^2q^2. \tag{3}$$

Let us notice that if $(p^2 + q^2)/2 - 2y^2 = 0$, we then get a right triangle with legs p and q and hypothenuse $2y$, which does not exist because both p and q are odd. Thus, we are lead to considering only the representations of p^2q^2 as a sum of two positive squares. We know, by Lemma 2.2 again, that the number of such representations (disregarding order) is 0 if both p

and q are $\equiv 3 \pmod 4$, it is $(d_1(p^2q^2)-1)/2 = 1$ if exactly one of p and q is $\equiv 3 \pmod 4$, and finally it is $(d_1(p^2q^2)-1)/2 = 4$ if neither p nor q is $\equiv 3 \pmod 4$. Since in the representation (3), the positive integer $2S$ is even (thus, $(p^2+q^2)/2-2y^2$ is odd), each such representation generates only two possible alternatives. When p (or q) is congruent to 1 modulo 4, we then write $p = u^2+v^2$ (or $q = z^2+w^2$) with u (respectively z) odd. The representations of p^2q^2 as $\big((p^2+q^2)/2-2y^2\big)^2+(2S)^2$ are

$$\big(p(z^2-w^2)\big)^2+(2pzw)^2, \tag{4}$$
$$\big(q(u^2-v^2)\big)^2+(2quv)^2, \tag{5}$$
$$\big((u^2-v^2)(z^2-w^2)+4uvzw\big)^2+\big((u^2-v^2)2zw-(z^2-w^2)2uv\big)^2, \tag{6}$$
$$\big((u^2-v^2)(z^2-w^2)-4uvzw\big)^2+\big((u^2-v^2)2zw+(z^2-w^2)2uv\big)^2. \tag{7}$$

In the case that both p and q are $\equiv 3 \pmod 4$, we have no nontrivial representation of p^2q^2 as a sum of two squares, therefore $H(p,q)=0$. If only one of these two primes is congruent to 1 modulo 4, then there is only one representation, namely either (4) or (5), according to whether $q \equiv 1 \pmod 4$, or $p \equiv 1 \pmod 4$, which then leads to the pair of equations (8) and (9), or (10) and (11) below, respectively. Thus, in this case $H(p,q) \le 2$. In the last and most interesting case when both p and q are $\equiv 1 \pmod 4$, each of the equations below could (at least at a first glance) produce an integer solution x_i (here, $x_i = 2y$):

$$p^2+q^2+2p(z^2-w^2) = x_1^2, \tag{8}$$
$$p^2+q^2-2p(z^2-w^2) = x_2^2, \tag{9}$$
$$p^2+q^2+2q(u^2-v^2) = x_3^2, \tag{10}$$
$$p^2+q^2-2q(u^2-v^2) = x_4^2, \tag{11}$$
$$p^2+q^2-2(u^2-v^2)(z^2-w^2)-8uvzw = x_5^2, \tag{12}$$
$$p^2+q^2-2(u^2-v^2)(z^2-w^2)+8uvzw = x_6^2, \tag{13}$$
$$p^2+q^2+2(u^2-v^2)(z^2-w^2)-8uvzw = x_7^2, \tag{14}$$
$$p^2+q^2+2(u^2-v^2)(z^2-w^2)+8uvzw = x_8^2. \tag{15}$$

To conclude the proof of Theorem 2.4, it suffices to show that if p and q are fixed, then at most five of the above eight equations can produce integer solutions x_i.

We first study the case when equation (8) has an integer solution x_1.

Lemma 2.5. *Assume that $q = z^2 + w^2$ with positive integers w and z, where z is odd. Then the prime p and the positive integer x_1 satisfy (8) if and only if $p = \frac{z^2}{\delta} + \frac{w^2}{\delta+1}$, where δ is a positive integer such that δ divides z^2 and $\delta + 1$ divides w^2.*

Proof. Let us prove the "if" part. Substituting the above expressions of p and q in terms of z^2 and w^2 into the equality (8), we get

$$p^2 + q^2 + 2p(z^2 - w^2) = z^4 \left(\frac{1}{\delta^2} + \frac{2}{\delta} + 1 \right) + w^4 \left(\frac{1}{(\delta+1)^2} - \frac{2}{(\delta+1)} + 1 \right)$$
$$+z^2w^2 \left(\frac{2}{\delta(\delta+1)} + 2 + \frac{2}{\delta+1} - \frac{2}{\delta} \right) = z^4 \left(\frac{1+\delta}{\delta} \right)^2 + w^4 \left(\frac{\delta}{\delta+1} \right)^2 + 2z^2w^2$$
$$= \left(\frac{(\delta+1)z^2}{\delta} + \frac{\delta w^2}{\delta+1} \right)^2.$$

So, $x_1 = \dfrac{(\delta+1)z^2}{\delta} + \dfrac{\delta w^2}{\delta+1}$, which is an integer under our assumptions.

For the other implication, rewrite (8) as $(p + z^2 - w^2)^2 + (2zw)^2 = x_1^2$. Using the general form of Pythagorean triples, we may write

$$p + z^2 - w^2 = d(m^2 - n^2) \text{ and } 2zw = 2dmn, \text{ or} \tag{16}$$
$$p + z^2 - w^2 = 2dmn \text{ and } 2zw = d(m^2 - n^2), \tag{17}$$

for some nonzero integers $m, n, d > 0$, with m and n coprime and of opposite parities.

We first look at the instance (16). Since $dmn = zw > 0$, we may assume that both m and n are positive integers. Solving the above equation for m and substituting it into $p + z^2 - w^2 = d(m^2 - n^2)$ gives

$$p = w^2 - z^2 + dm^2 - dn^2 = \frac{(z^2 + dn^2)(w^2 - dn^2)}{dn^2}.$$

Since p is prime and $z^2 + dn^2 > dn^2$, we see that it is necessary that $dn^2 = (w^2 - dn^2)\delta$ and $z^2 + dn^2 = \delta p$ for some positive integer δ. The first relation can be equivalently written as $w^2\delta = (\delta + 1)dn^2$. Because δ and $\delta + 1$ are coprime, it follows that $\delta + 1$ divides w^2.

Similarly, solving for n in (16) and arguing as before, we obtain $\delta'(dm^2 - z^2) = dm^2$ and $w^2 + dm^2 = \delta' p$ for some positive integer δ'. From these relations, we get $(\delta+1)(\delta'-1)=\delta\delta'$, or $\delta'=\delta+1$. Hence, $z^2(\delta+1)=\delta dm^2$, which implies that δ divides z^2. We then get

$$p=w^2-z^2+dm^2-dn^2=w^2-z^2+\frac{z^2(\delta+1)}{\delta}-\frac{w^2\delta}{(\delta+1)}=\frac{z^2}{\delta}+\frac{w^2}{\delta+1},$$

which completes the proof of the lemma in this case.

We now look at the instance (17). If we denote by $s=m+n$ and $t=m-n$, then $p+z^2-w^2=d(s^2-t^2)/2$, and $2zw=dst$. Note that s and t are both odd and, in particular, $st\neq 0$ and d is even. As before, solving for s, we get $s=\dfrac{2zw}{dt}$, and substituting it into $p+z^2-w^2=d(s^2-t^2)/2$ we get $p=\dfrac{(2z^2+dt^2)(2w^2-dt^2)}{2dt^2}$, which implies, as before and since $2z^2+dt^2>dt^2$, that both $\mu(2w^2-dt^2)=2dt^2$ and $2z^2+dt^2=p\mu$ hold with some positive integer μ. Hence, $2w^2\mu=(\mu+2)dt^2$.

As before, solving now for t we get $t=\dfrac{2zw}{ds}$, and substituting it into $p+z^2-w^2=d(s^2-t^2)/2$, we arrive at $p=\dfrac{(ds^2-2z^2)(2w^2+ds^2)}{2ds^2}$. By a similar argument, we get $2w^2+ds^2=p\mu'$ and $2ds^2=\mu'(ds^2-2z^2)$ with some positive integer μ'. This implies that $(\mu'-2)ds^2=2\mu'z^2$. From these relations, we obtain $(\mu'-2)(\mu+2)(dst)^2=\mu\mu'4z^2w^2$. This shows that $\mu'=\mu+2$. Since z and w are of opposite parities, we get that μ is even. The conclusion of the lemma is now verified by taking $\delta=\mu/2$. $\square$

Remark 1. *Similar statements hold for relations* (9)–(11)*, as well.*

We now give a numerical example.

Example 1. *Let s and t be positive integers such that both $p=3t^2+2s^2$ and $q=9t^2+4s^2$ are prime numbers. If we write $x_1=6(s^2+t^2)$, then the triangle with sides (p,q,x_1) is Heron, and x_1 satisfies equation (8).*

Another interesting example is $p=5$ and $q=1213=27^2+22^2$, which gives $z=27$ and $w=22$. In this case equation (9) is satisfied with $x_2=1212$, which leads to the Heron triangle with sides $(5,1213,1212)$. We note that $\frac{27^2}{243}+\frac{22^2}{242}=3+2=p$, which shows that $\delta=242$. This example shows that δ does not have to divide z or w.

We now record the following corollary to Lemma 2.5.

Corollary 2.6. *Assume that $q = z^2 + w^2$ is an odd prime. Then equations (8) and (9) cannot both have integer solutions x_1 and x_2.*

Proof. Assume, by way of contradiction, that both x_1 and x_2 are integers. Then, by Lemma 2.5, we must have

$$p = \frac{z^2}{\delta} + \frac{w^2}{\delta+1} = \frac{z^2}{\mu+1} + \frac{w^2}{\mu}$$

for some positive integers δ and μ satisfying the conditions from the statement of Lemma 2.5. If $\mu \geq \delta + 1$, then

$$\frac{z^2}{\mu+1} + \frac{w^2}{\mu} < \frac{z^2}{\delta} + \frac{w^2}{\delta+1}.$$

Similarly, if $\delta \geq \mu + 1$, we then have

$$\frac{z^2}{\mu+1} + \frac{w^2}{\mu} > \frac{z^2}{\delta} + \frac{w^2}{\delta+1}.$$

Thus, we must have $\delta = \mu$. But this is impossible because z and w have opposite parity. □

Corollary 2.7. *Assuming that both $p = u^2 + v^2$ and $q = z^2 + w^2$ are odd primes, then among the four equations (8), (9), (10) and (11), at most one of the x_i's is an integer ($i = 1, \dots, 4$).*

Proof. By way of contradiction, suppose that more than one of the x_i's is an integer. By Corollary 2.6, the number of such cannot exceed two. We now use Lemma 2.5 and obtain an integer δ with the property that either

$$p = \frac{z^2}{\delta} + \frac{w^2}{\delta+1} \qquad \text{or} \qquad p = \frac{w^2}{\delta} + \frac{z^2}{\delta+1}.$$

In either situation, we get $p < q$. Similarly, because one of equations (10) or (11) must have an integer solution, we must have either

$$q = \frac{u^2}{\delta'} + \frac{v^2}{\delta'+1} \qquad \text{or} \qquad q = \frac{v^2}{\delta'} + \frac{u^2}{\delta'+1},$$

which leads to $q < p$. This contradiction shows that at most one of the numbers x_i, $i = 1 \dots 4$, is an integer. □

This completes the proof of our Theorem 2.4. $\square$

We now give an example of an instance in which both equations (12) and (14) have integer solutions.

Proposition 2.8. *Both equations (12) and (14) have integer solutions if* $p = (ij)^2 + (kl)^2$ *and* $q = (ik)^2 + (jl)^2$ *for some positive integers* i, j, k *and* l *with* i, j, k *odd and* l *even.*

Proof. Since u and z are odd, we have $u = ij$, $v = kl$, $z = ik$ and $w = jl$. A straightforward calculation shows that

$$\begin{aligned}
&p^2 + q^2 - 2(u^2 - v^2)(z^2 - w^2) - 8uvzw \\
&= (i^2j^2 + k^2l^2)^2 + (i^2k^2 + j^2l^2)^2 - 2(i^2j^2 - k^2l^2)(i^2k^2 - j^2l^2) - 8i^2j^2k^2l^2 \\
&= (i^2j^2 - k^2l^2)^2 + (i^2k^2 - j^2l^2)^2 - 2(i^2j^2 - k^2l^2)(i^2k^2 - j^2l^2) \\
&= \left[(i^2j^2 - k^2l^2) - (i^2k^2 - j^2l^2)\right]^2 = (k^2 - j^2)^2(i^2 + l^2)^2 = x_5^2,
\end{aligned}$$

with $x_5 = |k^2 - j^2|(i^2 + l^2)$.

Similarly,

$$\begin{aligned}
&p^2 + q^2 + 2(u^2 - v^2)(z^2 - w^2) - 8uvzw \\
&= (i^2j^2 + k^2l^2)^2 + (i^2k^2 + j^2l^2)^2 + 2(i^2j^2 - k^2l^2)(i^2k^2 - j^2l^2) - 8i^2j^2k^2l^2 \\
&= (i^2j^2 - k^2l^2)^2 + (i^2k^2 - j^2l^2)^2 + 2(i^2j^2 - k^2l^2)(i^2k^2 - j^2l^2) \\
&= \left[(i^2j^2 - k^2l^2) + (i^2k^2 - j^2l^2)\right]^2 = (k^2 + j^2)^2(i^2 - l^2)^2 = x_7^2,
\end{aligned}$$

with $x_7 = |i^2 - l^2|(k^2 + j^2)$. $\square$

The examples below are of the type, which additionally satisfy three of the equations (12)–(15):

$p = 21521, q = 14969, x_1 = 14952, x_2 = 15990, x_3 = 33448,$
$p = 4241, q = 2729, x_1 = 1530, x_2 = 1850, x_3 = 6888,$
$p = 898361, q = 161009, x_1 = 952648, x_2 = 896952, x_3 = 870870,$
$p = 659137, q = 252913, x_1 = 512720, x_3 = 688976, x_3 = 722610,$
$p = 4577449, q = 11893681, x_1 = 11843832, x_2 = 14876232, x_3 = 10174630.$

We currently have no example satisfying all equations (12)–(15), at the same time.

Let us observe that the equations (12)–(15) are equivalent in the written order to

$$(u^2 - v^2 - z^2 + w^2)^2 + 4(uv - zw)^2 = x_5^2, \tag{18}$$

$$(u^2 - v^2 - z^2 + w^2)^2 + 4(uv + zw)^2 = x_6^2, \tag{19}$$
$$(u^2 - v^2 + z^2 - w^2)^2 + 4(uv - zw)^2 = x_7^2, \tag{20}$$
$$(u^2 - v^2 + z^2 - w^2)^2 + 4(uv + zw)^2 = x_8^2. \tag{21}$$

In particular, we have $H(p, q) \geq 2$ if $uv = zw$, or $u^2 - v^2 = z^2 - w^2$ or $u^2 - v^2 = w^2 - z^2$.

Theorem 2.9. *Assume that $q = z^2 + w^2$ is an odd prime, u, v, z and w are positive integers with both u and z odd and both v and w even. Then equation (21) has integer solutions if and only if there exist positive integers m, n, a and b with m and n coprime of opposite parities and a and b also coprime, such that a divides $nw - mz$, b divides $nz + mw$, and*

$$\begin{cases} u = nk - \frac{zb}{a} \in \mathbb{Z} \\ v = mk - \frac{wb}{a} \in \mathbb{Z}, \end{cases} \tag{22}$$

where $k = \frac{(a^2+b^2)(nz+mw)}{ab(n^2+m^2)}$.

Proof. For the sufficiency part, let us first calculate $u^2 - v^2 + z^2 - w^2$. We have, from (22),

$$u^2 - v^2 + z^2 - w^2 = (n^2 - m^2)k^2 - 2\frac{kb}{a}(nz - mw) + \frac{b^2}{a^2}(z^2 - w^2) + z^2 - w^2 =$$

$$(n^2 - m^2)k^2 - 2\frac{(a^2 + b^2)(n^2z^2 - m^2w^2)}{a^2(n^2 + m^2)} + \frac{(a^2 + b^2)(z^2 - w^2)}{a^2}.$$

This reduces to

$$u^2 - v^2 + z^2 - w^2 = (n^2 - m^2)k^2 - \frac{(a^2 + b^2)(n^2 - m^2)(z^2 + w^2)}{a^2(n^2 + m^2)} =$$
$$(n^2 - m^2)\left(k^2 - \tfrac{(a^2+b^2)(z^2+w^2)}{a^2(n^2+m^2)}\right).$$

On the other hand, $uv + zw = mnk^2 - \frac{kb}{a}(nw + mz) + \frac{b^2}{a^2}zw + zw$, which, as before, gives

$$uv + zw = mnk^2 - \frac{(a^2 + b^2)[(nz + mw)(nw + mz) - zw(n^2 + m^2)]}{a^2(m^2 + n^2)} =$$

$$= mn\left(k^2 - \frac{(a^2 + b^2)(z^2 + w^2)}{a^2(n^2 + m^2)}\right).$$

Putting these calculations together, we see that

$$(u^2-v^2+z^2-w^2)^2+4(uv+zw)^2 = (m^2+n^2)^2\left(k^2-\frac{(a^2+b^2)(z^2+w^2)}{a^2(n^2+m^2)}\right)^2.$$

This means that we can take x_8 in (21) to be $(m^2+n^2)k^2-(a^2+b^2)q/a^2$, which must be an integer since we assumed u and v were integers.

For the necessity part, let us observe that $(u^2-v^2+z^2-w^2)/2 \equiv 1 \pmod 2$ and $uv+zw \equiv 0 \pmod 2$, which imply that $u^2-v^2+z^2-w^2 = 2d(n^2-m^2)$ and $uv+zw = 2dmn$ for some nonzero integers m, n and $d > 0$, with m and n coprime and of opposite parities. From here, we see that $mn(u^2-v^2+z^2-w^2)-(n^2-m^2)(uv+zw) = 0$. This is equivalent to

$$mn(u^2-v^2)-(n^2-m^2)uv+mn(z^2-w^2)-(n^2-m^2)zw = 0,$$

or

$$(nu+mv)(mu-nv)+(nz+mw)(mz-nw) = 0. \tag{23}$$

We are now ready to define our coprime numbers a and b by the relation

$$\frac{a}{b} = \frac{nu+mv}{nz+mw}.$$

From here, we see that $nz+mw = bs$ for some integer s, and in light of (23) we also have

$$\frac{a}{b} = \frac{nw-mz}{mu-nv},$$

which shows that $nw-mz = as'$ for some integer s'. We are now going to show that both equalities in (22) hold. Indeed, let us look at the last two equalites as a system of linear equations with two unknowns in u and v:

$$\begin{cases} nu+mv = \frac{a}{b}(nz+mw), \\ mu-nv = \frac{b}{a}(nw-mz). \end{cases} \tag{24}$$

If one solves the above system for u and v, one gets exactly the two expressions in (22). □

Example: If $p = 113 = 7^2+8^2$, $q = 257 = 1^2+16^2$, which means that $u = 7$, $v = 8$, $z = 1$ and $w = 16$. Because $\frac{u^2-v^2+z^2-w^2}{uv+zw} = -15/4$, we get $n = 1$ and $m = 4$. Then $\frac{nu+mv}{nz+mw} = \frac{3}{5}$, which gives $a = 3$ and $b = 5$. Thus, $k = \frac{26}{3}$ and the formulae (22) are easily verified.

Theorem 2.10. *If $p = u^2+v^2$ and $q = z^2+w^2$ are odd distinct primes, with u, v, z and w as in Theorem 2.9 for which (21) has an integer solution x_8, then*

$$p + q = \ell(s^2 + s'^2), \tag{25}$$

where $nz + mw = sb$, $nw - mz = s'a$ and $a^2 + b^2 = \ell(m^2 + n^2)$ with integers s, s' and ℓ.

Proof. We apply Theorem 2.9 and obtain the numbers a, b, m, n and k with the specified properties. Using the above notations, we get $k = \dfrac{\ell s}{a}$. Squaring and adding together the equalities for u and v from Theorem 2.9, we get

$$p = u^2 + v^2 = (m^2 + n^2)k^2 - 2\frac{kb}{a}(nz + mw) + (z^2 + w^2)\frac{b^2}{a^2},$$

which becomes

$$p = \frac{(m^2 + n^2)\ell^2 s^2}{a^2} - 2\frac{b^2\ell s^2}{a^2} + q\frac{b^2}{a^2} = \frac{(a^2 + b^2)\ell s^2}{a^2} - 2\frac{b^2\ell s^2}{a^2} + q\frac{b^2}{a^2}.$$

Equivalently,

$$p + q = \ell s^2 + q\frac{a^2 + b^2}{a^2} - \frac{b^2\ell s^2}{a^2} = \ell s^2 + \ell\frac{(z^2 + w^2)(m^2 + n^2) - (nz + mw)^2}{a^2} =$$

$$= \ell s^2 + \ell\frac{(nw - mz)^2}{a^2} = \ell(s^2 + s'^2).$$

Let us show now that ℓ is an integer. Since we know that $u = nk - zb/a$ must be an integer, solving for nak we obtain that $n\frac{(a^2+b^2)s}{m^2+n^2} = nak = au + zb$ must be an integer as well. Since $\gcd(m^2 + n^2, n) = 1$, we see that $m^2 + n^2$ should divide $(a^2 + b^2)s$. The conclusion we want follows then provided that we can show that $m^2 + n^2$ and s are coprime. To this end, it is enough to prove that $\gcd(m^2 + n^2, nz + mw) = 1$.

By way of contradiction, assume that $m^2 + n^2$ does not divide $a^2 + b^2$ and there exists a prime number r which divides both $m^2 + n^2$ and $nz + mw$. Then r divides $n(nw - mz) = (m^2 + n^2)w - m(nz + mw)$. Because $\gcd(r, n) = 1$, we see that r must divide $nw - mz$. Hence, $nq = n(z^2 + w^2) = z(nz + mw) + w(nw - mz)$ is divisible by r. The assumption that q is prime together with the fact that $\gcd(r, n) = 1$ shows that $r = q$. In this case,

$m^2+n^2 = (z^2+w^2)(m_1^2+n_1^2)$ with $n = m_1 z - n_1 w$ and $m = n_1 z + m_1 w$ for some integers m_1, n_1. This gives $bs = nz + mw = m_1 q$.

On the other hand, the fact that m^2+n^2 divides $(a^2+b^2)(nz+mw)$ is equivalent to saying that $m_1^2+n_1^2$ divides $(a^2+b^2)m_1$. The fact that $\gcd(m_1^2+n_1^2, m_1) = 1$ implies that $m_1^2+n_1^2$ divides a^2+b^2. So, the fraction $\frac{(a^2+b^2)(nz+mw)}{b(m^2+n^2)}$ can be simplified to $\frac{a's}{q}$. If in addition q divides a', then m^2+n^2 divides a^2+b^2, which we excluded. If q divides s, then from the identity $(m^2+n^2)(p+q) = (a^2+b^2)(s^2+s'^2)$ and the above observation, we get $q(p+q) = a'(q^2 s_1^2 + s'^2)$. But this implies that q divides s' as well, and after simplifying both sides by q we get that q divides p, which is a contradiction. $\square$

Corollary 2.11. *Under the assumptions of Theorem 2.10, we have*

$$p + q = \alpha^2 + \beta^2 \tag{26}$$

for some integers α and β.

Proof. We can apply Theorem 2.10, as well as the theory of Gaussian integers (or directly, by looking at the prime power factorization), to get that $\ell = \frac{a^2+b^2}{m^2+n^2}$ must be of the form $m_1^2 + n_1^2$ for some integers m_1 and n_1. The existence of α and β follows from the Fermat identity $(s^2+s'^2)(m_1^2+n_1^2) = (sm_1 + s'n_1)^2 + (sn_1 - s'm_1)^2$. $\square$

3 Counting Heron triangles

In this section, we prove the following theorem.

Theorem 3.1. *The estimate*

$$\sum_{a,b\le x} H(a,b) < x^{25/13+o(1)} \tag{27}$$

holds as $x \to \infty$.

For the proof of the above result, we will use the following completely explicit two dimensional version of the Hilbert's Irreducibility Theorem due to Schinzel and Zannier [14], whose proof is based on results of Bombieri and Pila [3].

Lemma 3.2. *Let $\Phi \in \mathbb{Q}[t,y]$ be a polynomial irreducible over $\mathbb{Q}$ of total degree $D \geq 2$. Then, for every positive integer $\delta < D$ and for every $T \geq 1$, the number of integer points (t^*, y^*) such that $\Phi(t^*, y^*) = 0$ and $\max\{|t^*|, |y^*|\} \leq T$ is bounded by*

$$(3D\Lambda)^{\Lambda+4}T^{3/(3(\delta+3))},$$

where $\Lambda = (\delta+1)/(\delta+2)$.

Proof. This is Lemma 1 on page 294 in [14]. □

Lemma 3.3. *Let $A,\ B,\ C,\ D$ and E be integers with $ADE \neq 0$. Then every irreducible factor of*

$$F(t,z) = At^4 - (Bz^2 + C)t^2 - (Dz+E)^2 \in \mathbb{Q}[t,z]$$

has degree at least 2 in t.

Proof. Assume that this is not so. Then there exists a factor of $F(t,z)$ of the form $t - f(z)$ for some $f(z) \in \mathbb{Q}[z]$. Thus,

$$Af(z)^4 - (Bz^2 + C)f(z)^2 - (Dz+E)^2 = 0 \tag{28}$$

identically. By looking at the degrees, it now follows easily that $f(z)$ is either linear or constant. If $f(z) = K$ is constant, then the coefficient of z in the above relation is $-2DE \neq 0$, which is a contradiction. Suppose now that $f(z)$ is linear. Since $f(z) \mid Dz+E$, we get that $f(z) = \lambda(Dz+E)$ for some nonzero rational λ. Substituting in (28), we get

$$A\lambda^4(Dz+E)^2 - \lambda^2(Bz^2+C) - 1 = 0,$$

which is impossible as the coefficient of z is $2\lambda^4 ADE \neq 0$. □

Proof of Theorem 3.1. We proceed in several steps.

Notations.

We assume that $a,\ b$ and c are the sides of a Heron triangle Δ of surface area S opposing the angles $A,\ B$ and C, respectively. Since $ab\sin(C) = 2S \in \mathbb{Z}$ and $\cos(C) = (a^2+b^2-c^2)/(2ab) \in \mathbb{Q}$, we get that both $\sin(C)$ and $\cos(C)$ are rational. Furthermore, $\sin(C) = 2S/(ab)$. We let $a_{1,c}b_{1,c}$ be the denominator of the rational number $\sin(C)$ such that $a_{1,c} \mid a$ and $b_{1,c} \mid b$. Since $a_{1,c}b_{1,c}$ is a sum of two coprime squares, it follows that each one of $a_{1,c}$ and $b_{1,c}$ is also a sum of two coprime squares. We then write

$$a_{1,c}^2 = U^2 + V^2 \qquad \text{and} \qquad b_{1,c}^2 = W^2 + Z^2,$$

with some integers $U,\ V,\ Z$ and W such that $\gcd(U,V) = \gcd(W,Z) = 1$, $U \not\equiv V \pmod 2$ and $Z \not\equiv W \pmod 2$. Furthermore, up to interchanging W and Z and changing the signs of some of $U,\ V,\ W$ and/or Z, we may assume that

$$\sin(C) = \frac{UZ - VW}{a_{1,c}b_{1,c}} \qquad \text{and} \qquad \cos(C) = \frac{UW + VZ}{a_{1,c}b_{1,c}}.$$

Thus, we get that if we write $a_{2,c} = a/a_{1,c}$ and $b_{2,c} = b/b_{1,c}$, then

$$\begin{aligned} c^2 &= a^2 + b^2 - 2ab\cos(C) \\ &= a_{2,c}^2(U^2 + V^2) + b_{2,c}^2(W^2 + Z^2) - 2a_{2,c}b_{2,c}(UW + VZ) \\ &= (a_{2,c}U - b_{2,c}W)^2 + (a_{2,c}V - b_{2,c}Z)^2. \end{aligned} \qquad (29)$$

Furthermore, by Pythagoras, we know that $a_{1,c} = u^2+v^2$, therefore $\{U,V\} = \{|u^2 - v^2|, 2uv\}$ and similarly $b_{1,c} = w^2 + z^2$, therefore $\{W,Z\} = \{|w^2 - z^2|, 2wz\}$ for some integers $u,\ v,\ w$ and z with $\gcd(u,v) = 1,\ \gcd(w,z) = 1$, $u \not\equiv v \pmod 2$ and $w \not\equiv z \pmod 2$.

In a similar way, we get two more equations satisfied by our triangle of the same shape as (29), obtained by circularly permuting $a,\ b$ and c (and C, A and B, respectively).

From now on, we let x be a large positive real number. We assume that Δ is a Heron triangle of sides $a,\ b$ and c satisfying $\max\{a,b,c\} \le x$.

Triangles having large $a_{2,b}$.

Here, we assume that Δ is such that

$$\min\{a_{2,b},\ a_{2,c},\ b_{2,a},\ b_{2,c},\ c_{2,a},\ c_{2,b}\} \ge x^{4/5}. \qquad (30)$$

Then $a_{1,c}b_{1,c} = ab/(a_{2,c}b_{2,c}) \le x^{2/5}$. Since $a_{1,c}b_{1,c} = K^2+L^2$ for some coprime positive integers K and L such that

$$\sin(C) \in \{2KL/(K^2 + L^2),\ |K^2 - L^2|/(K^2 + L^2)\},$$

we get that $K < x^{1/5}$ and $L < x^{1/5}$. Thus, C can be chosen in $O(x^{2/5})$ ways. Similarly, there are only $O(x^{2/5})$ choices for B. Since $a \le x$, and since a side and its two adjacent angles determine the triangle uniquely, we get that the number of possible triangles in this case is $O(x^{9/5})$.

From now on, we count only those Heron triangles Δ which do not fulfill condition (30). To fix ideas, we assume that

$$a_{2,c} = \min\{a_{2,b},\ a_{2,c},\ b_{2,a},\ b_{2,c},\ c_{2,a},\ c_{2,b}\},$$

and that $a_{2,c} < x^{4/5}$. Furthermore, to simplify notations, from now on we will drop the subscript c. Relation (29) becomes

$$c^2 = (a_2U - b_2W)^2 + (a_2V - b_2Z)^2. \tag{31}$$

The case when $a_2V = b_2Z$.

Fix a_2. Then $a_1 = u^2 + v^2 \le x/a_2$, leading to $|u| \le (x/a_2)^{1/2}$ and $|v| \le (x/a_2)^{1/2}$. Thus, there are only $O(x/a_2)$ possibilities for the pair (u,v). Since V is determined by the pair (u,v), that is, $V \in \{|u^2 - v^2|, 2uv\}$, it follows that there are only $O(x/a_2)$ possibilities for V. Now $a_2V = b_2Z$, therefore both b_2 and Z divide a_2V. If $Z = 2wz$, then both w and z divide a_2V, while when $Z = |w^2 - z^2|$, then both $w - z$ and $w + z$ divide a_2V. In either case, we get that the number of possibilities for the triple (b_2, w, z) is $O(\tau(a_2V)^3) = x^{o(1)}$. It is now clear that c is uniquely determined once $a_2,\ u,\ v,\ b_2,\ w$ and z are determined as $c = |a_2U - b_2W|$. This argument shows that the number of possibilities for Δ in this case is

$$\le \sum_{a_2 < x^{4/5}} \frac{x^{1+o(1)}}{a_2} = x^{1+o(1)} \sum_{a_2 < x^{4/5}} \frac{1}{a_2} = x^{1+o(1)}.$$

A similar argument applies for the number of Heron triangles Δ with $a_2U = b_2W$.

From now on, we assume that $a_2V \ne b_2Z$ and that $a_2U \ne b_2W$. By relation (31), the three numbers $c,\ |a_2U - b_2W|$ and $|a_2V - b_2Z|$ form a Pythagorean triple with c as hypothenuse. Thus, there exist positive integers $d,\ M$ and N with M and N coprime and of different parities such that

$$\begin{aligned} &c = d(M^2 + N^2) \quad \text{and} \\ &\{\,|a_2U - b_2W|, |a_2V - b_2Z|\,\} = \{\,d|M^2 - N^2|, 2dMN\,\}. \end{aligned} \tag{32}$$

We shall only assume that

$$U = u^2 - v^2, \qquad V = 2uv, \qquad W = w^2 - z^2, \qquad Z = 2wz, \tag{33}$$

and

$$a_2U - b_2W = d(M^2 - N^2) \qquad \text{and} \qquad a_2V - b_2Z = 2dMN, \tag{34}$$

since the remaining cases can be handled similarly.

We now take κ_0 to be a positive constant to be determined later.

Triangles with large d.

We assume that $d > x^{\kappa_0}$. Then $M^2 + N^2 < x^{1-\kappa_0}$, therefore $|M| < x^{(1-\kappa_0)/2}$ and $|N| < x^{(1-\kappa_0)/2}$. Thus, the pair (M, N) can be chosen in $O(x^{1-\kappa_0})$ ways. We shall now fix a_2, u and v. This triple can be fixed in $x^{1+o(1)}$ ways (first we fix $a \le x$, then we fix $a_2 \mid a$ and u and v such that $u^2 + v^2 \mid a$). Dividing the last two equations (34) side by side and using equation (33), we get the equation

$$\frac{a_2(u^2 - v^2) - b_2(w^2 - z^2)}{a_2uv - b_2wz} = \frac{M^2 - N^2}{MN}.$$

Cross multiplying and reducing modulo b_2, we get that

$$b_2 \mid MNa_2(u^2 - v^2) - a_2uv(M^2 - N^2). \tag{35}$$

We now distinguish the following cases.

Case 1. $MNa_2(u^2 - v^2) - a_2uv(M^2 - N^2) = 0$**.**

Then $(u^2 - v^2)/(uv) = (M^2 - N^2)/(MN)$, and u and v are coprime. Thus, $uv = MN$, giving only $x^{o(1)}$ possibilities for the pair (u, v) once the pair (M, N) is fixed. Thus, if we first fix $c \le x$ and then $d \mid c$ and $M^2 + N^2 \mid c$, we see that there are $x^{1+o(1)}$ possibilities for the triple (d, M, N). Further, once d, M and N are fixed, the pair (u, v) can be chosen in only $x^{o(1)}$ ways. Finally, a_2 is fixed in $O(x^{4/5})$ ways. Thus, the number of ways to fix the pair (a, c) in this case is $x^{9/5+o(1)}$, and since b can take only $x^{o(1)}$ ways once the sides a and c are determined, we get that the number of such Heron triangles Δ is $x^{9/5+o(1)}$.

Case 2. $MNa_2(u^2 - v^2) - a_2uv(M^2 - N^2) \neq 0$**.**

Then b_2 can be chosen in $x^{o(1)}$ ways once (a, M, N) are fixed. Furthermore, we now get

$$b_2MN(w^2 - z^2) - b_2(M^2 - N^2)wz = MNa_2(u^2 - v^2) - a_2uv(M^2 - N^2). \quad (36)$$

Thus, there are $O(x^{2-\kappa_0})$ choices for the triple (a, M, N) in this case, and then b_2 is fixed in only $x^{o(1)}$ ways. Once b_2, d, M and N are fixed, equation (36) becomes

$$g(w, z) = K,$$

where K is fixed and nonzero and $g(w, z)$ is the quadratic form

$$Aw^2 + Bwz + Cz^2,$$

where

$$A = b_2MN, \qquad B = -b_2(M^2 - N^2) \qquad \text{and} \qquad C = -b_2MN.$$

The discriminant of g is

$$b_2^2((M^2 - N^2)^2 + 4M^2N^2) = b_2^2(M^2 + N^2)^2,$$

which is a nonzero perfect square. It now follows easily that the resulting equation (36) has only $x^{o(1)}$ possible solutions (w, z). Hence, the number of Heron triangles Δ is in this case $x^{2-\kappa_0+o(1)}$.

A similar count will show that the number of Heron triangles with $b_2 > x^{\kappa_0}$ is $x^{2-\kappa_0}$. Thus, we may assume that both b_2 and d are smaller than or equal to κ_0. Since $a_2 \le b_2$, we also get that $a_2 \le x^{\kappa_0}$.

Triangles with a_2, b_2 and d small.

We now assume that

$$\max\{a_2, b_2, d\} \le x^{\kappa_0}.$$

Using (33) and expressing w versus z from the second equation (34) and inserting it into the first, we get

$$a_2^2u^4 - (-a_2b_2z^2 + a_2b_2w^2 + a_2d(M^2 - N^2))u^2 - (b_2wz + dMN)^2 = 0. \quad (37)$$

Fix d, a_2 and b_2. Then $c = d(M^2 + N^2) \le x$, therefore we get $|M| \le (x/d)^{1/2}$ and $|N| \le (x/d)^{1/2}$. In a similar vein, $b = b_2(z^2 + w^2)$, therefore $|w| \le (x/b_2)^{1/2}$, and $|z| \le (x/b_2)^{1/2}$. Finally, $|u| \le (x/a_2)^{1/2}$. Thus, if the triple (d, a_2, b_2) is fixed, then the parameters (M, N, w) can be fixed in $O(x^{3/2}/(d\sqrt{b_2}))$ ways. Now equation (37) becomes an equation of the type $f(u, z) = 0$ in the variables u and z alone, where $f(t, x) \in \mathbb{Q}[t, x]$ is a polynomial of the form appearing in Lemma 3.3 with

$$A = a_2^2, \quad B = -a_2 b_2, \quad C = a_2 b_2 w^2 + d(M^2 - N^2), \quad D = b_2 w, \quad E = dMN.$$

Furthermore, u and z satisfy $\max\{|u|, |z|\} \le (x/a_2)^{1/2}$. Since obviously $ABD \neq 0$ for our polynomial, by Lemma 3.3, it follows that we can take $\delta = 1$ in Lemma 3.2, and get that the number of such solutions for a fixed choice of coefficients is

$$\ll \left(\frac{x}{a_2}\right)^{1/3}.$$

Hence, for fixed d, a_2 and b_2 the number of choices is

$$\ll \frac{x^{11/6}}{d b_2^{1/2} a_2^{1/3}}.$$

Summing the above relations up for $d \le x$, $a_2 \le x^{\kappa_0}$ and $b_2 \le x^{\kappa_0}$, we get that the number of Heron triangles in this case is

$$\begin{aligned} &\ll x^{11/6} \sum_{b_2 < x^{\kappa_0}} \frac{1}{b_2^{1/2}} \sum_{a_2 < x^{\kappa_0}} \frac{1}{a_2^{1/3}} \\ &\ll x^{11/6} \int_1^{x^{\kappa_0}} \frac{dt}{t^{1/2}} \int_1^{x^{\kappa_0}} \frac{dt}{t^{1/3}} \\ &\ll x^{11/6} \cdot x^{(1/2+2/3)\kappa_0} = x^{11/6 + 7\kappa_0/6}. \end{aligned}$$

Optimizing, we get $11/6 + 7\kappa_0/6 = 2 - \kappa_0$, therefore $\kappa_0 = 1/13$, which leads to the desired conclusion. $\square$

Acknowledgements. The authors would like to thank Yuri Bilu, Pierre Debes, Yann Walkowiak and Umberto Zannier and the anonymous referee for useful suggestions. During the preparation of this paper, F. L. was supported in part by grant SEP-CONACyT 46755 and by a Guggenheim Fellowship. The paper was written while P.S. was with Auburn University Montgomery.

References

[1] A. H. Beiler. Recreations in the Theory of Numbers: The Queen of Mathematics Entertains. New York: Dover, 1966.

[2] K.D. Boklan. *Problem* 11134. Am. Math. Monthly **112** (2005), 180.

[3] E. Bombieri, J. Pila. *The number of integral points on arcs and ovals.* Duke Math. J. **59** (1989), 337–357.

[4] Y.-G. Chen, S.-G. Guo. *On the rational cuboids with a given face.* J. Number Theory **112** (2005), 205-215.

[5] S.D. Cohen. *The distribution of Galois groups and Hilbert's irreducibility theorem.* Proc. London Math. Soc. **43** (1981), 227–250.

[6] R. K. Guy. Unsolved Problems in Number Theory. New York, Springer-Verlag, 290–291, 2000.

[7] H. Harborth, A. Kemnitz. *Fibonacci Triangles.* In Applications of Fibonacci Numbers, Volume 3 (Pisa, 1988), Dordrecht: Kluwer Acad. Publ., 1990, 129–132.

[8] H. Harborth, A. Kemnitz, N. Robbins. *Non-Existence of Fibonacci Triangles.* Congr. Numer. **114** (1996), 29–31.

[9] M. Huxley. *A note on polynomial congruences.* Recent Progress in Analytic Number Theory, Vol. I, Academic Press, 1981, 193–196.

[10] A.-V. Kramer, F. Luca. *Some Remarks on Heron Triangles.* Acta Acad. Paedagog. Agriensis, Sect. Mat. (N.S.) **27** (2000), 25–38.

[11] F. Luca. *Perfect Cuboids and Perfect Square Triangles.* Math. Mag. **73** (2000), 400–401.

[12] F. Luca. *Fermat Primes and Heron Triangles with Prime Power Sides.* Am. Math. Monthly **110** (2003), 46–49.

[13] K. Rosen. Elementary Number Theory and Its Applications. Addison Wesley, 512–514, 2005.

[14] A. Schinzel, U. Zannier. *The least admissible value of the parameter in Hilbert's Irreducibility Theorem.* Acta Arith. **69** (1995), 293–302.

[15] J.-P. Serre. Lectures on the Mordell-Weil Theorem (3rd Ed.). Aspects in Mathematics, E15, Vieweg, 1997.